

# **Table of Contents**

## **PART I. DISCOVERY OF ELECTRONIC EVIDENCE**

### **CHAPTER 1. INTRODUCTION**

#### **A. TEXT**

- § 1:1 What is electronic evidence?
- § 1:2 Use of forensic experts
- § 1:3 Contracting with litigation support companies and forensic specialists
- § 1:4 Outsourcing legal services
- § 1:5 An introduction to computers and computer networks

#### **B. FORMS**

- § 1:6 Example information security language for forensics expert agreement security
- § 1:7 Litigation support agreement
- § 1:8 Service levels and performance standards

### **CHAPTER 2. SOURCES OF ELECTRONIC EVIDENCE**

#### **A. TEXT**

- § 2:1 Overview
- § 2:2 Networks and workstations
- § 2:3 Removable disks
- § 2:4 USB Fobs and other removable media
- § 2:5 Temporary files
- § 2:6 Swap files
- § 2:7 Mirror disks
- § 2:8 Program files
- § 2:9 Embedded or metadata information
- § 2:10 Audit trails and computer logs
- § 2:11 Access control lists
- § 2:12 Electronic data interchange
- § 2:13 Internet related information
- § 2:14 Geolocation data

- § 2:15 Corporate intranets
- § 2:16 E-mail
- § 2:17 Ephemeral messaging
- § 2:18 Laptops and home computers
- § 2:19 Mobile phones
- § 2:20 PCMCIA memory cards
- § 2:21 Archival data: backups and other removable media
- § 2:22 Recoverable data
- § 2:23 Discovery of non-textual material
- § 2:24 Disaster recovery facilities
- § 2:25 Outsource vendors
- § 2:26 BYOD programs
- § 2:27 Federal guidelines for searching and seizing computers

## **B. FORMS**

- § 2:28 Checklist for handling electronic evidence
- § 2:29 Checklist of sources of electronic evidence

# **CHAPTER 3. OBTAINING ELECTRONIC EVIDENCE**

## **A. TEXT**

- § 3:1 Discovery overview
- § 3:2 Demands for inspection, copying, testing, or sampling of documents and other physical evidence: An overview
- § 3:3 Document demands
- § 3:4 Responding to document demand
- § 3:5 Demands for inspection of other physical evidence
- § 3:6 Subpoenas
- § 3:7 Motion to compel; sanctions
- § 3:8 Discovery sanctions
- § 3:9 Scope of discovery and limitations
- § 3:10 Documents stored on remote computers
- § 3:11 Special interrogatories
- § 3:12 Requests for admissions
- § 3:13 Depositions
- § 3:14 Exchange of expert witness information
- § 3:15 Protective orders
- § 3:16 Preservation requests and orders
- § 3:17 Use of technology in conducting discovery
- § 3:18 Data dumps
- § 3:19 Federal guidelines for searching and seizing computers

## TABLE OF CONTENTS

### § 3:20 References

## **B. FORMS**

- § 3:21 Sample document demands
- § 3:22 Example request for document production
- § 3:23 Sample points and authorities supporting application to compel production of documents and computer
- § 3:24 Example response to motion to compel
- § 3:25 Special interrogatories
- § 3:26 Requests for admissions
- § 3:27 Request for physical inspection
- § 3:28 Sample notice of deposition
- § 3:29 Sample deposition outline
- § 3:30 Preservation order
- § 3:31 Preservation order
- § 3:32 Exemplar Stipulated ESI Discovery Order

## **CHAPTER 4. OPEN RECORDS STATUTES**

### **A. TEXT**

- § 4:1 Access to government records
- § 4:2 Public Records Act
- § 4:3 Freedom of Information Act

### **B. FORMS**

- § 4:4 Public Records Act request
- § 4:5 Freedom of information request

## **CHAPTER 5. LIMITS ON DISCOVERABILITY**

### **A. TEXT**

- § 5:1 Overview
- § 5:2 Attorney-client privilege
- § 5:3 Work product doctrine
- § 5:4 Trade secrets and other proprietary information
- § 5:5 Copyright and license restrictions on the discoverability of electronic evidence
- § 5:6 Social media and the Stored Communications Act
- § 5:7 ESI specific objections

### **B. FORMS**

- § 5:8 Confidentiality agreement

- § 5:9 Sample notice letter to requesting party
- § 5:10 Sample notice letter to copyright owner

## **CHAPTER 6. RECORDS RETENTION/E-DISCOVERY**

### **A. TEXT**

- § 6:1 The benefits of an effective records retention policy
- § 6:2 Developing an effective records retention policy
- § 6:3 Developing an E-Discovery Policy
- § 6:4 Checklist for effective records retention policy
- § 6:5 Checklist for effective E-Discovery Policy
- § 6:6 Components of an effective records retention policy
- § 6:7 Checklist

## **CHAPTER 7. SPOILIATION OF EVIDENCE**

### **A. TEXT**

- § 7:1 Electronic document retention
- § 7:2 Duty to preserve ESI evidence in anticipation of litigation; “litigation hold”
- § 7:3 Spoliation of evidence and discovery sanctions
- § 7:4 Continuing viability of the tort of spoliation of evidence
- § 7:5 Sarbanes–Oxley and document retention
- § 7:6 References

### **B. FORMS**

- § 7:7 Preservation letter
- § 7:8 Suspension of document destruction procedures

## **CHAPTER 8. PRIVACY ISSUES**

### **A. TEXT**

- § 8:1 Constitutional privacy rights
- § 8:2 Common law invasion of privacy
- § 8:3 Statutory privacy provisions
- § 8:4 Privacy rights in litigation
- § 8:5 Employee privacy
- § 8:6 Social Media

### **B. FORMS**

- § 8:7 Employee computer use policy

TABLE OF CONTENTS

§ 8:8 Computer use memo

## **PART II. ADMISSIBILITY OF ELECTRONIC EVIDENCE**

### **CHAPTER 9. AUTHENTICATION OF ELECTRONIC EVIDENCE**

#### **A. TEXT**

- § 9:1 In general
- § 9:2 Audit trails
- § 9:3 Encryption authentication
- § 9:4 Intermediary transmission
- § 9:5 References

#### **B. FORMS**

- § 9:6 Example direct examination

### **CHAPTER 10. THE SECONDARY EVIDENCE RULE/BEST EVIDENCE RULE**

#### **A. TEXT**

- § 10:1 Secondary Evidence Rule replaces Best Evidence Rule
- § 10:2 What is an “original”?
- § 10:3 Printed representations of electronic documents
- § 10:4 Images on video or digital media
- § 10:5 References

#### **B. FORMS**

- § 10:6 Example direct examination

### **CHAPTER 11. HEARSAY RULE**

#### **A. TEXT**

- § 11:1 Introduction
- § 11:2 Operative fact doctrine
- § 11:3 Admissions
- § 11:4 Business and official records
- § 11:5 Qualifying the authenticating witness
- § 11:6 References

## **B. FORMS**

- § 11:7 Checklist of authentication issues for the business records exception
- § 11:8 Example direct examination

## **CHAPTER 12. ELECTRONIC PRESENTATIONS AT TRIAL**

### **A. TEXT**

- § 12:1 Computer generated visual evidence
- § 12:2 Types of CGVE
- § 12:3 When to consider using CGVE
- § 12:4 Admissibility of CGVE—In general
- § 12:5 Admissibility of computer animations
- § 12:6 Limiting instructions to the jury
- § 12:7 References

### **B. FORMS**

- § 12:8 Checklist of potential objections to CGVE
- § 12:9 Checklist of key authentication issues

## **CHAPTER 13. COMPUTER FORENSIC INVESTIGATIONS**

- § 13:1 Introduction
- § 13:2 Preparing for a case
- § 13:3 Identifying potentially obtainable and case-relevant evidence
- § 13:4 Ensure discovery requests are properly framed and limited
- § 13:5 The forensic investigation (*method, equipment, evidence control and handling*)
- § 13:6 Client actions that can negatively impact the case
- § 13:7 Certified investigator vs. Certified examiner vs. Court examiner
- § 13:8 Questions to ask a prospective computer forensics expert

## **CHAPTER 14. A TRIAL COURT JUDGE'S PERSPECTIVE ON ELECTRONIC EVIDENCE DECISION-MAKING**

- § 14:1 Age-old protocols for new-age evidence
- § 14:2 Understanding the nature of the judge as an “audience/decision-maker”

## TABLE OF CONTENTS

- § 14:3 The judge's over-arching role: gate-keeper
- § 14:4 The RASH approach
- § 14:5 Building an advocacy arsenal to assist the judge in ruling on evidentiary issues related to electronic evidence
- § 14:6 Parting "wisdom" for parties and attorneys seeking judicial understanding of electronic evidence

## APPENDICES

- Appendix A. List of Internet Search Engines
- Appendix B. Freedom of Information Act (including Electronic Freedom of Information Act Amendments of 1996)
- Appendix C. Selections from the Electronic Communications Privacy Act of 1986
- Appendix D. California State and Local Bodies Required to Have Public Records Act Guidelines
- Appendix E. Federal Experts For Computer Crime Investigations
- Appendix F. Discovery of Computerized Data, Manual for Complex Litigation
- Appendix G. Federal Guidelines For Searching And Seizing Computers (And Supplement)
- Appendix H. Best Practices For Seizing Electronic Evidence
- Appendix I. Computer Crime And Intellectual Property Section
- Appendix J. ESI Discovery—Statutory authority and other informational resources
- Appendix K. California Electronic Evidence Rules
- Appendix L. California Electronic Discovery Act
- Appendix M. 2011 California Senate Bill No. 1574, California 2011-2012 Regular Session
- Appendix N. National Institute of Justice, Special Report Electronic Crime Scene Investigation: A Guide for First Responders
- Appendix O. Federal Trade Commission Guidelines
- Appendix P. U.S. District Court E-Discovery (ESI) Guidelines

### Table of Laws and Rules

### Table of Cases

### Index